

「2007年度の情報セキュリティ政策の評価等」 について

※ 第17回情報セキュリティ政策会議(平成20年4月22日)資料

2008年5月13日

内閣官房情報セキュリティセンター(NISC)

<http://www.nisc.go.jp>

「次期
情報セキュリティ
基本計画」

「第1次情報セキュリティ基本計画」(2006年2月2日 情報セキュリティ政策会議)



2006年度 → 2007年度 → 2008年度

「セキュア・ジャパン2006」
(2006年6月15日 情報セキュリティ政策会議)

- 2006年度の実施計画
～「官民におけるセキュリティ対策の体制の構築」
- 2007年度の重点施策の方向性
～「官民におけるセキュリティ対策の底上げ」

「セキュア・ジャパン2007」
(2007年6月14日 情報セキュリティ政策会議)

- 2007年度の実施計画
～「官民におけるセキュリティ対策の底上げ」
- 2008年度の重点施策の方向性
～「セキュリティ基盤強化に向けた集中的取組み」

「セキュア・ジャパン2008」

- 2008年度の実施計画
～「情報セキュリティ基盤の強化に向けた集中的な取組み」
- 2008年度の重点施策の方向性
～「持続的な情報セキュリティ対策の推進体制の構築に向けた基盤整備」

報告

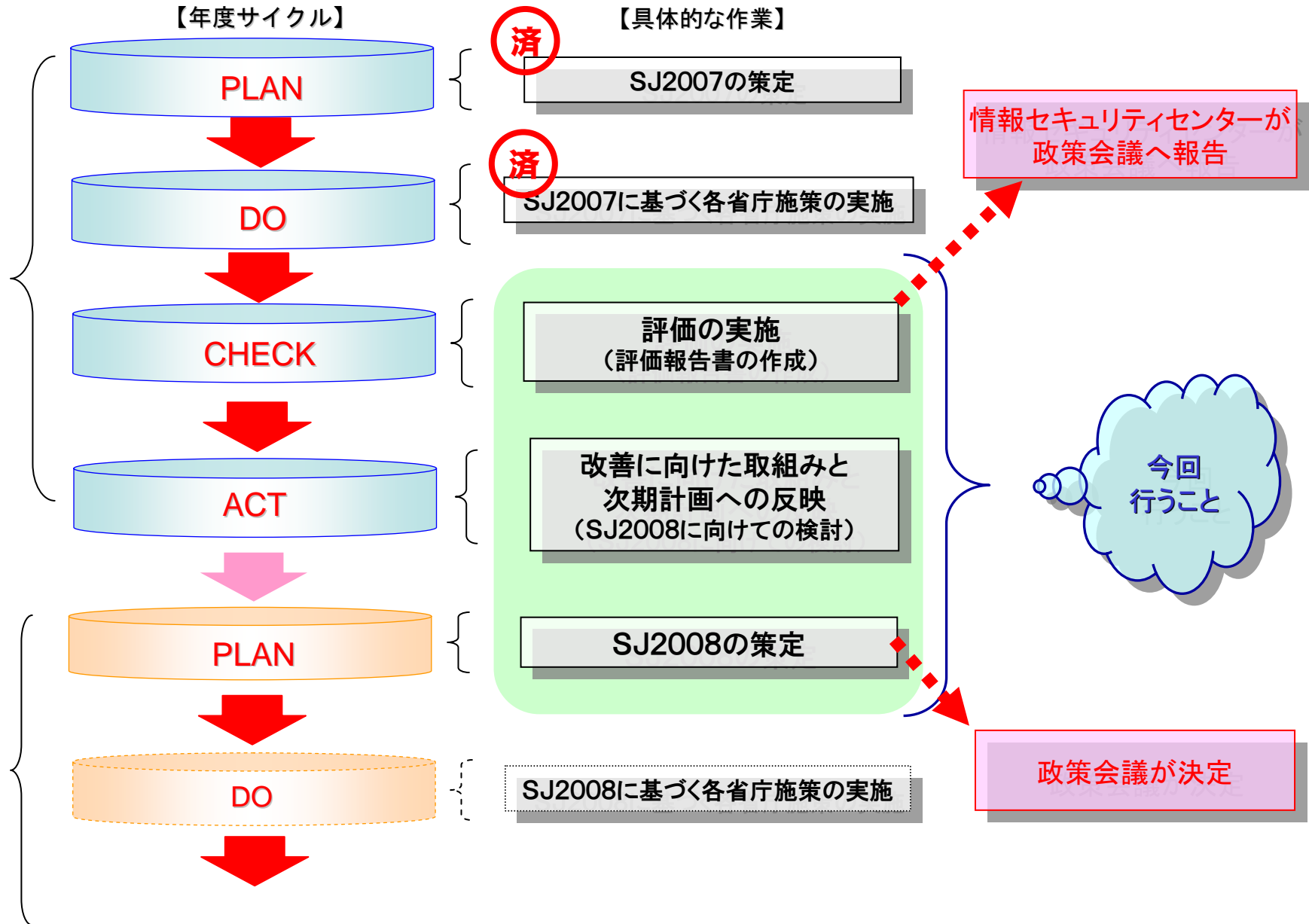
**2006年度の
評価等**
2007年4月23日 内閣官房
情報セキュリティセンター

報告を受け止める形で政策会議として現状を認識・評価

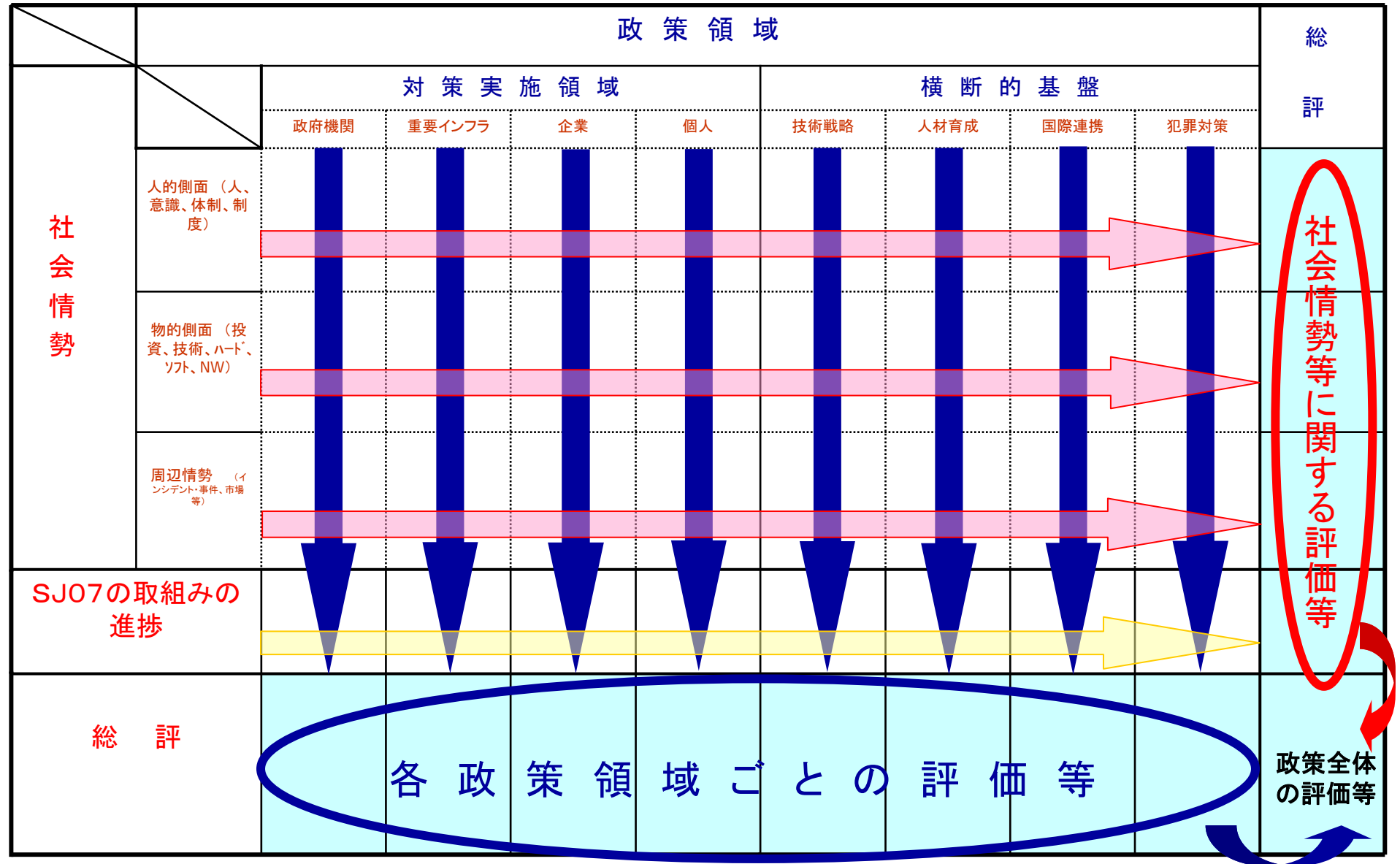
報告

**2007年度の
評価等**
2008年4月22日 内閣官房
情報セキュリティセンター

報告を受け止める形で政策会議として現状を認識・評価



※検討の主眼は情報セキュリティ政策が社会に与えた変化や情報セキュリティに関連のある事象を網羅的に把握することではなく、SJ2008の検討に有益な情報をできるだけ多く検討すること



○ 情報セキュリティ政策全体(総評)

- ・官民の情報セキュリティ対策のための体制維持、対策推進の安定化へ向けた取組みが懸命に進められた。
- ・各対策実施領域の取組み状況に一定の進展があり、「官民における情報セキュリティ対策の底上げ」も進んだものと考えられる。
- ・情報セキュリティに関するリスクの大幅な軽減はみられず、情報セキュリティ政策の社会的効果は十分な判断がつかない状況。
- ・現行技術水準の限界もあると考えられ、対策水準の向上には体制の強化、効率的な対策の推進が引き続き求められる。

○ 2007年度の取組み及び取組みを受けた現状の評価等

■ SJ2007に盛り込まれた取組み

第一次基本計画及びSJ2007の目標に掲げられる「4つの基本方針」に対する取組み

(1) 官民各主体の共通認識の形成

⇒ 官民各主体の共通認識の強化

- ・政府機関の持続的改善構造による対策推進意識の高まり
- ・重要インフラ10分野CEPTOAR整備完了、安全基準等の見直し、官民連携による分野横断的演習、相互依存性解析、情報共有体制の強化へ向けた継続的な取組み等を通じた対策推進意識の高まり
- ・教育拠点、教育ツールの整備、教育事業者団体の業界横断的な連携体制の構築等、官民における人材育成に係る意識の浸透

(2) 先進的技術の追求

⇒ 先進的技術の追求の継続

- ・政府全体として情報セキュリティ分野へ重点投資を進める環境の整備
- ・ボットを使ったサイバー攻撃等の課題を解決する技術等、課題解決型の技術開発の推進

(3) 公的対応能力の強化

⇒ 政府機関対応体制の確立の推進

政府機関に対するサイバー攻撃等に関する横断的な情報収集・分析・情報共有を行うための体制(GSOC※)整備開始

※Government Security Operation Coordination Team

(4) 連携・協調の推進

⇒ 連携協調へ向けた活動の開始、NISCを結節点とした連携(各主体間の横断的連携はこれから)

国際協調・貢献に関する基本方針の策定を受けた本格的な活動の開始

重要インフラ10分野CEPTOARの連携、情報共有体制CEPTOAR-Council(仮称)の創設へ向けた検討等

■ SJ2007の取組みの状況と成果

2007年度の一年間の取組みの状況と成果としては、

- 1) 各主体における情報セキュリティ意識の維持・強化
- 2) 対策実施領域ごとの具体的取組みの着実な推進
- 3) 横断的な情報セキュリティ基盤分野における具体的取組みの着実な推進
- 4) 情報セキュリティ推進体制の維持・強化と持続的改善構造に基づく政策の推進、であったと言える。

○ 政府機関(総評)

・政府機関の対策は2006年度と比較し一定の成果が見られるものの、対策が不十分な部分や課題が残っている結果となり、目標達成に向けた取り組みが必要である。

①対策実施状況報告により、教育の実施、格付け、システム台帳の整備、等の課題が残っていることが分かった。教育等の重要な課題が2006年度に続いて不十分な状態にあることは、重大な問題と言わざるを得ない。今後、改善に向けた取組みを加速する必要がある。

②端末及びウェブサーバについて重点検査を実施したところ、昨年と比較して対策実施状況に大きな改善が見られ、各府省庁における対策が着実に向上していると認められた。引き続き、更なる改善に向けた取組みが必要である。

○ 2007年度の取組み及び取組みを受けた現状の評価等

対策実施状況

政府機関全体で約30万人分の対策実施状況報告を基に、政府機関における情報セキュリティ対策の実施状況を把握・分析

⇒ 平均把握率: 93.4%、平均実施率: 93.4%

平均到達率: 100%実施した割合 = 64.1%、95%以上実施した割合 = 75.8%、90%以上実施した割合 = 81.7%

特筆すべき遵守事項の全府省庁の平均実施率

情報セキュリティ対策の教育: 84.2%、格付け・取扱い制限に係る措置: 89.7%、情報システム台帳の整備: 77.9%、

安全区域内における職員識別の実施: 93.2%

重点検査状況

「政府機関の情報セキュリティ対策のための統一基準」 端末・ウェブサーバ・電子メールサーバの基本遵守事項の検査

H19年3月末時点

⇒ 端末 対策実施率100% 8府省庁(全19府省庁中) 80%以上100%未満 11府省庁(全19府省庁)

(H18年 対策実施率100% 0府省庁、80%以上100%未満 4府省庁、60%以上100%未満 10府省庁、60%未満 6府省庁)

⇒ ウェブサーバ 対策実施率100% 9府省庁(全19府省庁中) 80%以上100%未満 10府省庁(全19府省庁中)

(H18年 対策実施率100% 1府省庁、80%以上100%未満 14府省庁、60%以上100%未満 14府省庁)

H19年9月末時点

⇒ 電子メールサーバ 対策実施率100% 10府省庁(全19府省庁中) 80%以上100%未満 9府省庁(全19府省庁中)

情報セキュリティマネジメント

政府機関の優れた取組み 44件選定 うち5件をベストプラクティスとして選定

一般職員の情報セキュリティ教育受講の推進

政府機関統一基準とそれに基づく評価・勧告によるPDCAサイクルの構築

政府統一基準の見直しの実施－政策会議16回会合にて、第三版を決定

PDCAサイクルの確立－職員への教育についての取組み、情報セキュリティ対策の実施状況の自己点検を実施

政府機関における安全な暗号利用の促進

危殆化に係るハッシュ関数移行指針の検討

サイバー攻撃等に対する政府機関における緊急対応能力の強化

政府機関に対するサイバー攻撃等に関する横断的な情報収集・分析・情報共有のための体制-GSOCの整備開始

○ 重要インフラ(総評)

- ・ 行動計画に基づく取組みを推進。その成果として、個々の重要インフラ事業者等による情報セキュリティ対策の向上を確認。
- ・ 情報共有については、体制等の整備・充実は着実に進んだものの、活発な運用にはなお時間を要する。
- ・ IT利用は引き続き進展や拡大が予想され、IT障害を発生させる要因や脅威は常に変化し続けることから、対策向上へ向けた継続的取組みが必要。

○ 2007年度の取組み及び取組みを受けた現状の評価等

安全基準等の整備

- ・ 安全基準等の見直し－H19年6月に行われた指針(「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」(2006年2月2日情報セキュリティ政策会議決定))の改定を踏まえ、重要インフラ10分野全てにおいて、9月末までに「安全基準等」の見直しを実施
- ・ 事業者等への浸透状況調査－H18年度に策定・見直しを行った各重要インフラ分野における安全基準等について実施
→ 安全基準等の認知率 97.9%、見直し率54.8%(2,958事業者(回収率96.2%))
- ・ 指針の見直し－H18年度に続いて分析・検証を実施、見直しの要点を重要インフラ10分野に周知する参考資料としてとりまとめ

情報共有体制の強化

- ・ CEPTOAR整備の推進－新規追加3分野(水道、医療、及び物流)において2007年度までに整備完了予定 → 10分野全てで完了
CEPTOARを構成する事業者数：5,692事業者(10分野、14CEPTOAR)
- ・ 情報共有訓練・分野横断的演習の実施、及びCEPTOAR特性把握マップ(Ver.2)のとりまとめ
- ・ 重要インフラ連絡協議会(CEPTOAR-Council)(仮称)の設置に向けた検討
－CEPTOAR代表者などから構成される「重要インフラ連絡協議会(CEPTOAR-Council)(仮称)創設に向けた検討の場」を設け8回の会合及び5回のワーキングを実施。「CEPTOAR-Council(仮称)の創設についての基本的な考え方」としてとりまとめ

相互依存性解析及び分野横断的演習の実施

- ・ 相互依存性解析－重要インフラ事業者間の相互依存関係の存在を確認。
- ・ 分野横断的演習－緊急時における情報共有・情報連絡について、具体的事象を想定したシナリオにより実施。
NISC、重要インフラ所管省庁、重要インフラ事業者等、CEPTOARがプレイヤーとして参加
要した年間延べ時間(1,768時間) 延べ参加者数(120名)

○ 企業(総評)

- ・ 対策、体制の強化が徐々に進められている状況であり、対策の重要性に係る意識も向上している。
- ・ 対策の著しい伸びはみられず、投資は、経済的損失との比較衡量の下で、各主体の経営判断によってなされる傾向と推察
- ・ 「取組み効果が認識しづらい」、「最低限これだけは取り組めば良いという事項が見えない」との指摘、一部に「対策疲れ」の声もある。
- ・ 先進的企業と、規模が小さい企業の間において、意識格差が生じているのではないかとの懸念もある。
- ・ 現行の対策枠組みの下で、取組み推進の「均衡点」に到達しつつあるとも考えられ、また、現行技術水準で守ることのできるセキュリティの「限界点」に到達している可能性もある。

○ 2007年度の主な取組み

企業の情報セキュリティ対策が市場評価につながる環境の整備

情報セキュリティ地策に係るベストプラクティス普及の方策、情報セキュリティ格付けの促進の方策のための調査研究
情報セキュリティ管理を重視した情報サービスマネージメントに関する標準化の取組み
－ JISQ20000-1/JISQ20000-2 の制定

中所企業向け標準フォーマットの策定へ向けた現状調査等の調査研究

質の高い情報セキュリティ関連製品及びサービスの提供促進

情報セキュリティ対策による情報セキュリティ関連リスクの変動を定量的に把握する手法の調査研究

オフショア・アウトソーシングに関連するリスクの検討(オフショア・アウトソーシングの現状に係る調査研究)

各種セミナーによる監査制度の普及活動、保証型情報セキュリティ監査の検討の継続的实施

情報セキュリティ関連製品等の普及促進の取組み

－ 認証製品の活用可否を確認する検討支援ツール、「情報基盤強化税制」、「ネットワークセキュリティ維持税制(地方税)」等の税制優遇措置の実施

企業における情報セキュリティ人材の確保・育成

「情報通信人材研修事業支援制度」による研修事業への助成

IT利用者の情報セキュリティを客観的に測定するセルフチェックツールの機能拡張

セキュリティ人材も含めた高度IT人材に求められるスキルの継続検討、実践的な高度IT人材育成方法の検討

ICTマネージメント分野の実践的なPBL(Project Based Learning)教材の開発

情報処理技術者試験制度においてH21年から新試験を実施予定

中小企業向け情報セキュリティセミナー(IPA/日本商工会議所)の開催

コンピュータウイルスや脆弱性等に早期に対応するための体制の強化

情報セキュリティ早期警戒パートナーシップ関連ガイドラインの改定・公開

早期警戒情報の共有ツールの稼動(重要インフラ10分野中、8分野を含む諸団体が利用)

共通脆弱性評価システムのVer2への移行(IPA)、JPCERT/CC 脆弱性優先度判定のためのシステム公開

Webアプリケーション構築の際の受注者へ示すべきセキュリティ要件に関するガイドラインを開発

○ 個人(総評)

- ・ **総体的**には、情報セキュリティに対する**意識の向上等が着実に進められている**が、基本的と思われる対策も含め、その必要性の認識や対策実施の**さらなる向上及び改善**が望まれる。個人の**属性間に意識、対策状況の格差**。**格差是正を含めた全体の底上げ**が更に求められる。
- ・ 被害に係る具体的なイメージがわからない、内容が難しすぎると思う者も多数。脅威などの**新たな変化**を踏まえ、**属性を考慮したわかりやすい形での普及啓発・情報発信**が必要。

○2007年度の主な取組み

情報セキュリティ教育の強化・推進

小中高等学校における情報セキュリティ教育推進 教員向けWebサイト作成
各都道府県 市区町村教育委員会指導主事等を対象とした情報モラル指導セミナーを開催
小学生・中学生・高校生対象「情報セキュリティ標語・ポスター」の募集・入選作品の公表 (IPA)
ICTメディアリテラシー育成プログラムの公開・更新
教員ICT活用指導力チェックリストに「児童生徒に対して情報セキュリティを指導する能力」を含め、全国の実態調査を実施
「インターネット安全教室」、「e-ネットキャラバン」、「サイバーセキュリティカレッジ」の実施を継続、普及・啓発の推進

広報啓発・情報発信の強化・推進

Webサイト「@police」のアプリケーションなどの脆弱性、新種コンピュータウィルスの発生に係る注意喚起等の広報啓発
「国民のための情報セキュリティサイト」の更新内容の検討
「インターネット美化運動2007」、「CHECK PC!キャンペーン」を実施、情報セキュリティの重要性を訴える活動
「迷惑メールへの対応の在り方に関する研究会」におけるフィッシングメール対策に関する検討
不正アクセスの発生状況及びアクセス制御機能に関する研究開発の状況の公表
JPCERT/CC、IPAによる情報管理者を対象とした不正アクセス対策、コンピュータウィルス対策等についての啓発活動
電波利用秩序の維持のための啓発活動
ホームページ、メールマガジン等の各種手段を用いた情報セキュリティに関する広報啓発・情報発信活動の推進
「情報セキュリティの日」に伴う広報啓発活動、各種関連行事の開催(593件)、功労者表彰
情報強化月間「情報化促進貢献表彰(情報セキュリティ促進部門)」期間集中的な広報啓発・情報発信活動の推進
我が国の情報セキュリティ戦略の国内外への発信 「基本計画」、「SJ2007」、「統一基準」のNISC英語サイト掲載

個人が負担感なく情報関連製品・サービスを利用できる環境整備

ボットプログラム感染を防ぐ対策、感染コンピュータからの攻撃停止の対策検討
IPv6による、少数かつ特定の利用者が存在する利用環境モデル(小規模オフィス環境等)での実証実験
無線LAN利用ガイドライン「安心して無線LANを利用するために」を改定
「インターネット安全教室」冊子改定、無線LANの安全な使い方に関するコンテンツの充実

○ 情報セキュリティ技術戦略の推進

- ・ 政府全体として情報セキュリティ分野への重点投資を進める環境整備が進展しつつある。
- ・ 「高セキュリティ機能を実現する次世代OS環境の開発」では、中間成果をβ版としてオープンソース化するなど着実な進展。ボットを使ったサイバー攻撃等の課題を解決するための技術開発等、課題解決型の技術開発も数多く実施。
- ・ 組織・人間系の管理手法の高度化に対する取組みにおいては十分に実施されたとは言えず、課題となる施策が存在することも事実。
- ・ 2007年度に構築した「研究開発・技術開発の効率的な実施体制」、「グランドチャレンジ型」研究開発・技術開発の一層の推進が必要。

○ 情報セキュリティ人材の育成・確保

- ・ 「人材育成・資格制度体系化専門委員会」の報告を受け、セキュリティ人材の育成に向けて官民における取組みを展開、展開を通じた人材育成の広まり、意識の浸透。
- ・ 政府による教育拠点や教育ツールの整備が図られるなど、人材育成に資する体制・基盤の整備が進展。
- ・ 民間分野では、セミナー開催やキャリアパスの検討等の枠組みを超えた業界横断的な取組みを推進する連携体制が整備された。
- ・ 他方、教育機会を活用し、実際の「情報セキュリティ人材」が組織内で技能を発揮するには時間を要し、発展の途上といえる。

○ 国際連携・協調の推進

- ・ 国際会議への参加や国際会議ワークショップの開催提案を通じ、議論過程への積極関与を行った。国際会議等における取組み紹介やウェブサイトによる広報活動を通じ、日本の取組みの認知度は向上(窓口としての認識)。
- ・ 情報セキュリティ領域での我が国発の国際貢献へ向けた基本方針*を策定し、国際連携・協調に向けた取組みを本格化。さらに取組みの具体化を図ることが課題。
※情報セキュリティ政策会議決定「我が国の情報セキュリティ分野における国際連携・協調へ向けた取組み」(平成19年10月3日)
- ・ 国際連携・協調へ向けた政策提言を開始したところであり、提言の実現に向けた継続的な働きかけが重要。

○ 犯罪の取締り及び権利利益保護・救済

- ・ 捜査能力や体制の構築については、一定の取組みができたが、技術開発は途上。取組みを継続し、加速化させる必要がある。
- ・ 一定の取組みがなされているものの、サイバー空間での犯罪や不法行為が多発している状況。権利利益の保護・救済についても、対応が十分とは言えない。インターネットの利用に不安を感じる人が半数に近いとの調査もあり、対策の一層の強化が必要。

○ 社会情勢 [人的側面(人材、意識、体制・制度)]

- ・ **人材面**では、人材の育成・確保に向けた官民の積極的な取組みの展開を通じた体制・基盤の整備が図られ、社会全体としての人材の育成に関する意識が浸透し始めた。様々な機会を活用した、社会のニーズに応える十分な人材育成・確保にはなお時間を要す。取組みは発展の途上と言える。
- ・ **意識面**では、SJ2007に基づく各種の取組みの推進、マスコミ報道(重要情報の漏えいや基盤となるITシステムの障害の報道等)、不正アクセス行為やネットワーク利用犯罪の増加傾向など、各々の対策実施領域での情報セキュリティに係る意識は徐々に高まっているものと考えられる。
- ・ **体制面**では、全般的には具体的な取組み推進のための枠組み構築が徐々に進められた一年。
 - 政府機関** : 対策推進の努力が懸命に続けられるものの、更なる対策水準の向上には体制強化への更なる取組みが必要。
 - 重要インフラ** : 事業継続性の確保を軸に置いた、情報共有、連絡・連携を進めるための枠組み・体制は徐々に構築されつつある。
 - 企業** : ISMS認証取得事業者数の着実な伸びなど、組織的な対応を含む対策、体制の強化の取組みが徐々に進められている。

○ 社会情勢 [物的側面(投資、技術、ハード、ソフト、ネットワーク)]

- ・ **投資面**は、昨年度から大幅な変化はないものの、必要なものについては堅実な投資を、対策を着実に行おうとしている状況にあると言える。
 - 政府機関** : 政府機関に対するサイバー攻撃等に関する横断的な情報収集・分析・情報共有のための体制整備の開始、政府機関統一基準遵守にかかわるシステム構築予算の昨年度比同水準の確保
 - 企業** : 情報セキュリティの技術的対策への投資は、経済的損失との比較衡量の下で、各主体の経営判断でなされる傾向と推察
 - 個人分野** : 全体としての底上げは図られていると考えられるが、年代別・男女別の格差。必要な対策ソフトの入手をはじめ、更なる対策実施状況の向上が望まれる。
- ・ **技術面**は、研究開発・技術開発の様々な取組みが着実に進められている状況にあり、取組みの成果によって、セキュリティを確保する技術の限界水準が現在と比べて向上し、対策が大幅に進むことが期待される。

○ 社会情勢 [周辺情勢(インシデント・事件、市場等)]

- ・ 情報流出やIT障害は依然として続き、また不正アクセス行為、ネットワーク利用犯罪も増加傾向にあり、情報セキュリティに係るリスクが低減しているとは言いがたい状況。
- ・ 経済的利得を狙った攻撃が発生するなど、依然として攻撃の目的、手段は変化し、被害が顕在化しにくくなる傾向にある。

○施策の実施状況

A : 予定どおり施策を推進することができた施策	… 144施策(90.6%)
B+ : 年度内には完了していないが、着実に取組みを進めており、数ヶ月以内には完了する施策	… 1施策(0.6%)
B : 予定どおり推進することができなかったが、今後も取組みを続けることにより最終的には施策を推進することができる施策	… 12施策(7.5%)
C : 予定どおり施策を推進することはできず、今後の見通しも立たない施策	… 1施策(0.6%)
— : 予定どおり施策を推進することができなかったが、その理由が政府機関の事情によるものではない施策	… 1施策(0.6%)

「A」とされた施策について

144施策(90.6%)について予定どおり施策を推進。内5施策については施策は推進するも、体制・人員に関して課題があるため、継続的な推進に当たって解決が必要であることが、作業の進捗や各省へのヒヤリング等から明らかになった。これら5施策については、政府機関の対策実施に関する取組みであり、政府機関の情報セキュリティ対策推進のための、体制や人員の不足が課題であることがうかがえる。

施策は推進されたが、体制・人員に関して課題があり、継続的な推進に当たって解決が必要な5施策

- ・各政府機関でのPDCAサイクルの定着
- ・政府全体でのPDCAサイクルの定着
- ・対策実施状況に関する評価等
- ・情報セキュリティマネジメントに関する評価等
- ・情報セキュリティ対策の体制の強化及び府省庁横断的な取組みの実施

「B+」とされた施策について

各府省庁で「IT人材育成・確保実行計画」を作成をしており、数ヶ月以内には全府省庁で完了する見込み。

「B」とされた施策について

情報資産台帳の整備や「go.jp」ドメインへの移行など全府省庁が実施すべき施策であったものの、一部府省庁で実施が完了しなかったものが6施策、その他、刑事共助条約の締結等、施策を推進したものの年度内に完了できなかったものが6施策となっている。

全府省庁が実施すべき6施策

- ・各府省庁の情報システムの一元的把握
- ・政府機関のドメイン名であることが保証されるドメイン名の利用の促進
- ・情報セキュリティマネジメントシステム適合性評価制度等の活用
- ・情報セキュリティ監査制度の活用
- ・安全性・信頼性の高いIT製品等の利用推進
- ・入札条件等の見直し

その他の6施策

- ・電子政府認証ガイドライン利用の推進
- ・「情報システムの信頼性向上に関するガイドライン」の活用・普及
- ・政府機関における安全な暗号利用の推進体制等の検討
- ・地方公共団体における情報セキュリティ対策の手引きの作成
- ・客観的な高度IT人材評価メカニズムの構築
- ・中央当局制度を活用した国際捜査共助の迅速化

「C」とされた施策について

本格的な電子政府運用開始に向けたOS等システム導入における技術動向調査について、既存OS環境でのセキュリティレベルの向上や現在開発中の高セキュリティ機能を実現する次世代OS環境の開発(セキュアVM)の成果をかんがみると、施策実施は不要と判断した。

「ー」とされた施策について

刑法等の改正(「犯罪の国際化及び組織化並びに情報処理の高度化に対処するための刑法等の一部を改正する法律案」)で、政府機関の事情以外の理由により完了しなかったものが1施策となっている。